

**CLAIMS:**

1. A method for protecting against unauthorized distribution of a copyrighted digital file by end-users over a peer-to-peer (P2P) network, said method comprising:
- 5 providing at least one corrupted copy of the copyrighted digital file on a first computer server; said at least one corrupted copy sharing sufficient similarities with said copyrighted digital file so as to be identifiable by at least one of the end-users as the copyrighted digital file;
- 10 connecting said first computer server to the P2P network; and allowing access to said at least one corrupted copy over the P2P network to said at least one of the end-users;
- whereby, copying of said at least one corrupted copy by said at least one of the end-users yields a version of said at least one corrupted copy which becomes available through the peer-to-peer network and identifiable as
- 15 the copyrighted digital file, thereby a) decreasing the probability that one of the end-users accesses the copyrighted digital file, b) diminishing the reliability of the peer-to-peer network, and c) contributing to dissuading unauthorized distribution of the copyrighted digital file over the peer-to-
- 20 peer network.
2. A method as recited in claim 1, wherein said at least one corrupted copy of the copyrighted digital file is selected from the group consisting of a truncated copy of the copyrighted digital file, a file including
- 25 information not included in the copyrighted digital file, a copy of the copyrighted digital file having a lesser quality than the copyrighted digital file, and a partially incomplete copy of said copyrighted digital file.

3. A method as recited in claim 1, wherein said at least one corrupted copy of the copyrighted digital file includes a truncated copy of the copyrighted digital file, or a corrupted content that does not correspond to the content of said copyrighted digital file.

5

4. A method as recited in claim 1, wherein the copyrighted digital file is selected from the group consisting of a computer application related file, a text file, a video file, a digital picture, a sound file, and a music file.

10

5. A method as recited in claim 1, wherein said at least one corrupted copy of the copyrighted digital file includes at least one file attribute not corresponding to any file attribute of the copyrighted digital file.

15

6. A method as recited in claim 1, wherein the copyrighted digital file is in the form of an audio file including music.

7. A method as recited in claim 6, wherein said at least one corrupted copy of the copyrighted digital file is in the form of an MPEG Audio Layer 3 (MP3) or a WAV file.

20

8. A method as recited in claim 6, wherein said at least one corrupted copy of the copyrighted digital file includes glitches or noises.

25

9. A method as recited in claim 8, wherein said glitches or noises is added to the copyrighted digital file after digitalisation thereof.

10. A method as recited in claim 1, further comprising connecting a second computer server to the peer-to-peer network; said second computer server querying the P2P network for a copy of the copyrighted file, and monitoring occurrences of copies of the copyrighted  
5 file among corrupted copies of the copyrighted file.

11. A method as recited in claim 10, wherein said at least one corrupted copy of the copyrighted digital file includes identification means allowing identification of said at least one corrupted copy of the  
10 copyrighted digital file by said second computer server.

12. A system for protecting against unauthorized distribution of a copyrighted digital file by end-users over a peer-to-peer (P2P) network using respective end-user device configured to share digital files over the  
15 P2P network, said system comprising: a first computer server connected to the peer-to-peer network; said first computer server including at least one corrupted copy of the copyrighted digital file; said at least one corrupted copy sharing sufficient similarities with the copyrighted digital file so as to be identifiable by at least one of the end-users as the copyrighted  
20 digital file.

13. A system as recited in claim 13, wherein said corrupted copy of the copyrighted digital file is selected from the group consisting of a truncated copy of the copyrighted digital file, a file including information  
25 not included in the copyrighted digital file, a copy of the copyrighted digital file having a lesser quality than the copyrighted digital file, and a partially incomplete copy of said copyrighted digital file.

14. A system as recited in claim 13, wherein said first computer server includes account information allowing access to the P2P network by said first computer server and access to said at least one corrupted version of the copyrighted digital file to at least one of said end-  
5 users.

15. A system as recited in claim 13, further comprising a second computer server connected to the peer-to-peer network; said second computer server being configured for querying the P2P network for  
10 the copyrighted digital file and for monitoring occurrences of the copyrighted digital file among corrupted copies of the copyrighted digital file.

16. A system as recited in claim 15, wherein said at least one  
15 corrupted copy of the copyrighted digital file includes identification means allowing identification of said at least one corrupted copy of the copyrighted digital file by said second computer server.

17. A system as recited in claim 13, wherein the copyrighted  
20 digital file is selected from the group consisting of a computer application file, a text file, a video file, a digital picture, a sound file, and a music file.

18. A system as recited in claim 13, wherein the copyrighted  
25 digital file is in the form of an audio file including music.

19. A system as recited in claim 13, wherein said at least one corrupted copy of the copyrighted digital file is in the form of an MPEG Audio Layer 3 (MP3) or a WAV file.

20. A system as recited in claim 13, wherein said corrupted copy of the copyrighted digital file includes glitches or noises.

5 21. A system as recited in claim 20, wherein said glitches or noises are added to the copyrighted digital file after digitalisation thereof.